AWARENESS BRIEF

Economic Espionage

Conducting Business in the International Marketplace

Editor's Note:

A previous CSIS Liaison / Awareness Brief *Economic Espionage: Clandestine Methods Used to Disadvantage Canadian Interests* (April 1998), identified some economic espionage methodologies used to disadvantage Canadian interests. The purpose of this brief is to highlight some of the economic security issues that impact upon individuals and organizations who conduct international business. The vulnerability of Canadian businesspeople to acts of economic espionage can be reduced through timely information about the practice of economic espionage in the international marketplace and the adoption of personal security practices.

This brief is published as part of CSIS's national Liaison/Awareness Program. Through this program, the Service seeks to establish ongoing dialogue with organizations, both public and private, concerning the threat posed to Canadian interests by foreign government involvement in economic espionage.

Introduction

With the international political and economic scene in constant flux, the target of espionage has changed. Economic espionage has become a very real threat that can emanate from any country. Many countries can and do use their state apparatus, including their intelligence resources, in the name of national economic competitiveness. In some instances foreign governments facilitate this espionage by turning a "blind eye" to these activities. State-owned and controlled corporations have also been implicated in economic espionage activities. The target of these intelligence resources and intelligence gathering activities include government officials, trade delegations, business executives and scientists. The effectiveness of these espionage activities are increased when they are practised against unwitting persons abroad.

Traditionally, neither business nor government took stock of the damage caused by economic espionage. However, recent private and public accounts of overseas incidents have highlighted that the financial cost may be in the hundred of millions of dollars. Non-financial damage to business can include public embarrassment for a company, the tarnishing of a corporate image, loss of business confidence from partners or shareholders and a public misconception that a company is a security risk because it cannot protect its sensitive information. One of the long-term effects of economic espionage is an erosion of a country's research and development base. The cost to develop new ideas and bring them to

fruition is capital intensive, and the loss of the resulting technology or research information surrounding just one project can be financially debilitating. Legal recourse can prove to be a lengthy and unrewarding experience that provides inadequate restitution. This can be particularly complicated, time-consuming and expensive if it is pursued through foreign jurisprudence.

Travelling

Overseas travel is a necessary component of everyday business for many companies. Business must seek out foreign markets and new buyers. Recognizing this fact, knowledge of some of the possible economic espionage scenarios one might face when travelling in a foreign country is helpful.

It is not always possible to know whether economic espionage is part of the business milieu of a country. Political and economic instability can aid in creating an atmosphere conducive to economic espionage. However, it is important to remember that all countries carry the potential for conducting economic espionage. Additionally, the level of sophistication available to industrialized countries in comparison to non-industrialized countries, rises dramatically.

Foreign countries have used their intelligence services to target the industrial and commercial companies of competing nations. Espionage is one venue toward gaining an effective advantage in the scientific and technological arena in addition to strengthening national economic interests. Public information has revealed that in some instance, countries gather this information on behalf of the state-owned corporations. Additionally, some state-owned corporations may practise economic espionage in their financial dealing at home and abroad.

Intelligence officers operating within the boundaries of their own country have the advantage of access to and cooperation amongst a wide network of local contacts. They also have enhanced knowledge of local geography and access to government support and resources when conducting clandestine targeting.

There are public statements that several countries maintain branches of their intelligence services to conduct economic espionage operations against foreign business and government personnel. Some of these statements include charges of collusion between the local telephone service and the national intelligence service. Many countries have the capacity to eavesdrop on transatlantic and transpacific communications, including phone and fax. Other means by which they can gain access to sensitive information is by covertly bugging and breaking into hotel rooms, hacking into computer databases, physically stealing computers, infiltrating personnel into companies, appealing to employee nationality, threats, coercion and bribery.

Any data can be targeted if it has an economic or strategic value. This can include sales data, client/supplier lists, technical drawings/details, research and development results, corporate planning documents, pricing documents or bidding strategies.

Travel Plans

When making plans to travel be aware that there is a possibility that a foreign intelligence service or a foreign interest, may have taken notice of your travel plans. Some countries monitor businesspeople of interest who travel overseas. Some competitors are interested in the overseas meetings that take place between businesspeople and prospective partners. Valuable information can be obtained through seemingly innocuous conversations that take place en route to a business destination. There are public reports of aircraft being bugged. Stewards may be overhearing conversations that they should not be privy to. An individual who takes an active interest in your company or its products may not simply be an overly inquisitive student or scientist. It is important to keep sensitive facts and details out of casual conversations with unknown individuals.

There are public allegations that some hotels and their staff have colluded with people committing economic espionage. In order to reduce the chance that your stay in a particular room might e the subject of unwanted attention, hotel arrangements can be made on your own and details kept confidential. If an unknown business contract is insistent on a particular hotel, or if you are unfamiliar with hotels in a particular city, it does not hurt to ask for two or three options.

Taxi drivers can be used as a source of information. Business discussions that take place in the back of a taxi are not necessarily secure. There is no guarantee that the driver is oblivious to the conversation or unknowledgeable about the language spoken. Some taxi drivers may be used to collect specific individuals from the airport or hotel for the specific purpose of overhearing or recording a sensitive conversation.

Transportation of Sensitive Documents

Many businesspeople carry sensitive documents and laptop computers with them when they travel. This can place their information in a vulnerable position. Documents can be photocopied or photographed when they are out of your possession. Laptop computers can have their files copied. Restaurants, hotels, foreign company offices, can all offer brief opportunities for documents or laptop computers to be compromised when left unattended.

The easiest solution is simply not to carry valuable information with you when you travel. If you must carry sensitive information with you, try to keep it small, concealed and easily stored on your person. Key information can be kept on a diskette or reduced to cue-card sized documents and enlarged later. Luggage checked onto an airline is vulnerable to interception. Unprincipled employees may search specific baggage for information or technology that they have been alerted to retrieve ahead of time.Packages sent overseas with commercial carriers can be the subject of interception by foreign interests practising economic espionage. Packages can arrive late, damaged or not at all. Packaging articles so that they cannot be tampered with is one option to detect and discourage targeting. Using a reliable and reputable carrier can also decrease the chance of tampering or interception. Sending bids by two independent carriers can reduce the possibility of a lost or delayed bid.

Business Contacts

Business contacts can come from all manner of sources. These contacts can be individuals met through trade shows or conferences, individuals introduced through business associates or simply individuals that have "cold called". It is always important to know a businessperson's bona fides. Unsolicited calls from contacts overseas should be researched and confirmed, including checking any references they provide. There have been examples of individuals from overseas "governments" appealing to Canadian business to provide business bank account numbers into which they could deposit money. Once the numbers are provided, the overseas "officials" take money from the account, not deposit money into it.

Businesspeople can be approached by foreign individuals at international trade shows on the pretext of purchasing their technology whin in fact, the individuals are interested in gaining detailed information on the company's inner-workings, its technology or its R&D. Keep track of all information and technology brought to a show. Keep it secured when attending to other enquiries. Any inquiry or request of a suspicious or unusual nature should be noted. These instances can prove valuable in forewarning other businesspeople to potential harm.

Overseas travellers must assume that hotel and conference rooms, as well as foreign business offices, are not secure areas within which one can discuss or divulge sensitive information. These rooms do not provide adequate security for unattended documents or laptop computers. Phones can be tapped and rooms can be monitored, clandestinely entered and searched. Scraps of paper of information that might be casually dumped into the trash can be retrieved to provide information on evolving business deals or contacts. Hotel safes may also be accessible to foreign intelligence services.

Communications

Many countries have very powerful electronic interception capabilities. Satellite communications can be intercepted by countries who monitor international communications. A limited series of prearranged words and codes for use over the phone or fax can allow a discussion of business matters between an overseas employee and a head office, if the need arises. Encryption systems for fax information and overseas communications gives greater security than open communications; however, even the use of these

systems does not offer complete security against foreign intelligence resources

Computers

Computers and electronic communications have become a mainstay of the business and government workplace. Computers store, transmit, retrieve and interpret large quantities of information and technological data. Internet and World Wide Web are playing an increasingly important role in connecting up computer users on the information highway. As such, they are also a sensitive and vulnerable target. Information stored in computers can be remotely accessed and retrieved from around the world via international communications links. These links can be intercepted and deciphered. Hackers can enter public and private sector databases. Modern-day technology even permits the retrieval of information previously erased from a computer's memory.

Conclusion

The national economic strength of a country is gauged in part by the health of its corporations and their ability to succeed in the global marketplace. A nation's ability to promote and protect its economic strength is as essential as its ability to defend itself. It is for these reasons that some foreign nations and their state corporations may find it more convenient to use their intelligence resources in pursuit of economic espionage against specific companies and personnel.

It is conceded that the vast majority of business conducted by Canadians in the overseas marketplace happens without incident. However, it is important to recognize that as the economic stakes in business rise, so too does the temptation to tilt the scales of equity. This document is designed to aid in forewarning and forearming Canadian business against such a possibility.

April 1998

103-00905/

Comments on this brief are welcome, and should be directed to the National Coordinator, Economic and Information Security, Box 9732, Station "T", Ottawa, K1G 4G4, phone (613) 231-0100, fax (613) 842-1390. If you'd like to talk to CSIS regarding a particular security concern, please contact the local Economic and Information Security Coordinator at one of the CSIS offices listed below:

Newfoundland ..... (709) 772-5449

Nova Scotia ..... (902) 420-5900

New Brunswick ..... (506) 452-3786

Quebec
- Montreal ..... (514) 393-5600
- Quebec City ..... (418) 529-8926

Ontario
- Ottawa ..... (613) 998-1679
- Toronto ..... (416) 865-1480

Manitoba ..... (204) 983-5405

Saskatchewan ..... (306) 780-5512

Alberta
- Edmonton ..... (403) 421-5800
- Calgary ..... (403) 292-5255

British Columbia ..... (604) 528-7400

BULLETIN DE SENSIBILISATION

Espionnage économique

Faire des affaires sur le marché international

Note de la rédaction :

Un bulletin précédent intitulé *Espionnage économique : Moyens clandestins employés au détriment des intérêts canadiens* (avril 1998), décrivait quelques-unes des méthodes préjudiciables aux intérêts du Canada utilisées dans le domaine de l'espionnage économique. Le présent bulletin met l'accent sur quelques-uns des aspects de la sécurité économique qui touchent les personnes qui font des affaires à l'échelle de la planète. Les gens d'affaires canadiens peuvent se prémunir contre l'espionnage économique s'ils sont renseignés à l'avance sur les subterfuges utilisés contre eux lorsqu'ils voyagent à l'étranger et s'ils prennent les mesures de sécurité adéquates pour se protéger.

Le présent bulletin est publié dans le cadre du Programme national de liaison et de sensibilisation du SCRS, dont l'objectif est d'établir avec les secteurs public et privé un dialogue permanent sur les menaces aux intérêts du Canada décrites ci-après l'espionnage économique animé par les gouvernements étrangers.

Introduction

Les cibles de l'espionnage varient au gré des fluctuations de la conjoncture politique et économique internationale. L'espionnage économique représente désormais une menace bien réelle à laquelle n'importe quel pays peut avoir recours. Nombreux sont ceux qui peuvent mettre leur appareil d'État et notamment les services secrets à contribution au nom de la compétitivité économique nationale et ne s'en privent pas. Certains gouvernements étrangers appuient tacitement l'espionnage en fermant les yeux sur les activités de ceux, entreprises d'État ou autres, qui s'y livrent. Personne n'est à l'abri de leurs menées; ils s'intéressent aussi bien aux représentants gouvernementaux qu'aux scientifiques, aux délégations commerciales qu'aux chefs d'entreprise. Leurs efforts sont encore plus fructueux quand ils agissent à l'insu de leurs cibles.

Jusqu'à tout récemment, ni les entreprises ni les gouvernements ne tenaient de statistiques sur les dommages causés par l'espionnage économique. Ce n'est plus le cas, puisque les rapports d'incidents survenus récemment à l'étranger tant dans le secteur privé que public révèlent que les pertes financières peuvent s'élever à plusieurs centaines de millions de dollars. Les entreprises subissent en outre des préjudices d'ordre moral, car ces opérations les mettent dans l'embarras, ternissent leur image de marque, minent la confiance de leurs partenaires commerciaux ou de leurs actionnaires et incitent la population à croire à tort qu'elles représentent un risque pour la

sécurité parce qu'elles ne peuvent protéger leurs secrets. À long terme, l'espionnage économique provoque, entre autres effets, une érosion des investissements dans le domaine de la recherche et du développement. Les coûts associés à la conception et à la concrétisation de nouvelles idées sont très élevés. Dès lors, le vol d'une nouvelle technologie ou des résultats des recherches effectuées dans le cadre d'un seul projet peuvent désormais décourager tout effort en ce sens. Les poursuites judiciaires, qui peuvent être longues et infructueuses, ne permettent jamais de compenser le préjudice subi. Le processus peut en outre se révéler particulièrement complexe, long et onéreux si les poursuites sont engagées à l'étranger.

Les voyages

Les voyages à l'étranger font partie intégrante du quotidien de nombreuses entreprises. Elles doivent chercher de nouveaux débouchés et de nouveaux clients. Il peut dès lors être utile de sensibiliser les gens d'affaires qui voyagent à l'étranger à quelques-uns des pièges de l'espionnage économique.

Il n'est pas toujours possible de savoir si le secteur industriel d'un pays recourt à l'espionnage économique, quoique l'instabilité politique et économique peut contribuer à créer un climat propice à ce type d'activité. L'important, c'est se rappeler que tous les pays sont susceptibles de s'y livrer, d'autant plus que le fossé entre les pays industrialisés et les pays en voie de développement ne cesse de s'élargir.

Les pays étrangers ont chargé leurs services de renseignements de prendre les secteurs industriels et commerciaux de leurs concurrents pour cible. L'espionnage est en effet l'un des moyens dont ils disposent pour damer le pion à leurs compétiteurs dans les secteurs techniques et scientifiques et consolider leurs intérêts économiques. D'après des sources d'information ouvertes, ces renseignements sont dans certains cas collectés pour le compte des entreprises d'État. Enfin, certaines d'entre elles peuvent avoir recours à l'espionnage économique dans leurs opérations financières, qu'elles soient menées sur le territoire national ou à l'étranger.

Les agents de renseignements actifs dans leur propre pays ont l'avantage d'avoir accès à un vaste réseau de contacts locaux et de pouvoir compter sur leur collaboration. Ils connaissent en outre mieux la géographie du pays et ils bénéficient du soutien et des ressources du gouvernement dans l'exécution de leurs missions secrètes.

Certains ont déclaré publiquement que dans plusieurs pays, une direction des services secrets est chargée de mener des opérations d'espionnage économique contre le personnel des entreprises et des gouvernements étrangers. D'autres ont même accusé la compagnie téléphonique locale et le service de renseignements national de collusion. De nombreux pays ont acquis la capacité d'intercepter les transmissions transatlantiques et transpacifiques, dont les communications téléphoniques et par télécopieur. Ils peuvent aussi mettre la main sur des renseignements sensibles en s'introduisant clandestinement dans les chambres d'hôtel et en y dissimulant des micros, en piratant les bases de données informatiques ou en volant les ordinateurs, en infiltrant des agents dans les entreprises ou encore en faisant vibrer la fibre nationaliste des employés ou en recourant à la menace, à la coercition et au chantage.

Toute information peut être utile si elle a une valeur économique ou stratégique. Il peut s'agir du chiffre d'affaires, de listes de clients et de fournisseurs, de dessins et de détails techniques, de résultats de travaux de recherche et de développement, de documents de planification générale ou sur l'établissement des prix ou encore de documents de stratégie relativement à des appels d'offres.

La planification des voyages

Un service de renseignements ou des intérêts étrangers peuvent être au courant des projets de voyage d'un homme ou d'une femme d'affaires à l'étranger. Certains pays surveillent en effet les gens d'affaires qui les intéressent et qui voyagent à l'étranger. Certains concurrents s'intéressent aux rencontres de gens d'affaires avec des partenaires potentiels à l'étranger. De précieux renseignements peuvent être obtenus au cours de conversations en apparence anodines qui se déroulent pendant le voyage. Des rapports publics

font état de micros dissimulés dans les avions. De plus, les agents de bord peuvent surprendre des conversations qui ne les concernent pas. Celui ou celle qui pose beaucoup de questions sur une entreprise ou ses produits n'est en définitive peut-être pas simplement un étudiant ou un scientifique trop curieux. Il est important de ne fournir aucun renseignement ou détail sensible au cours de conversations à bâtons rompus avec des inconnus.

Certaines personnes ont affirmé publiquement que des hôtels et leur personnel ont participé secrètement à des opérations d'espionnage économique. Pour limiter les risques que votre séjour dans une chambre donnée attire indûment l'attention, faites vous-mêmes vos réservations et gardez-en les détails confidentiels. Si un contact d'affaires inconnu insiste pour que vous descendiez dans un hôtel donné, ou si vous ne connaissez pas les hôtels d'une ville, prenez des renseignements sur deux ou trois d'entre eux.

Les chauffeurs de taxi peuvent servir d'informateurs. Vous ne pouvez donc pas être absolument sûr que vos conversations resteront secrètes. Rien ne vous permet en effet d'affirmer que le chauffeur n'écoute pas, et il ne faut pas tenir pour acquis qu'il ne comprend pas votre langue. Certains d'entre eux peuvent avoir précisément pour mission de prendre en charge certaines personnes à l'aéroport ou à un hôtel pour écouter ou enregistrer leur conversation.

Transport de documents sensibles

De nombreux hommes et femmes d'affaires transportent des documents secrets et des ordinateurs portatifs lorsqu'ils voyagent et risquent, ce faisant, d'en compromettre la sécurité. Leurs documents peuvent être photocopiés ou photographiés lorsqu'ils les laissent quelque part, et les fichiers mémorisés dans leur ordinateur portatif peuvent être copiés. Au restaurant, dans les hôtels et dans les bureaux des entreprises étrangères, quelqu'un peut avoir l'occasion, si brève soit-elle, de prendre connaissance de documents papier ou mémorisés dans un ordinateur portatif laissés sans surveillance.

Le plus simple est de ne transporter aucun renseignement sensible lorsque vous voyagez. Si c'est impossible, consignez-les sur un support de dimension réduite que vous pourrez dissimuler et transporter facilement sur vous. Vous pouvez les emmagasiner sur une disquette ou les noter sur des documents réduits à la dimension de fiches qui pourront être agrandis au besoin. Les bagages que vous confiez aux lignes aériennes ne sont pas en sécurité ; ils peuvent être interceptés. Des employés peu scrupuleux peuvent avoir été chargés de les fouiller pour trouver des informations ou des technologies bien précises.

Les colis envoyés à l'étranger par l'intermédiaire de services de messagerie commerciaux peuvent également être interceptés par les intérêts étrangers qui se livrent à l'espionnage économique. Ils peuvent être endommagés, livrés en retard ou ne pas l'être du tout. Il est possible d'emballer les envois de telle sorte qu'ils ne puissent être ouverts sans qu'on s'en rende compte, pour décourager ceux qui seraient tenter de le faire. Les risques peuvent en outre être minimisés par le choix d'un service de messagerie fiable et de bonne réputation. Enfin, en confiant ses soumissions à deux services différents, l'entreprise limite le risque qu'elles soient égarées ou livrées en retard.

Les contacts d'affaires

Vous pouvez rencontrer des contacts d'affaires en diverses occasions, par exemple lors de foires commerciales ou de conférences, ils peuvent vous être présentés par des collègues ou tout simplement entrer en relation avec vous à l'improviste. Il faut toujours vérifier la bonne foi de la personne. Les appels imprévus de contacts à l'étranger doivent être vérifiés et confirmés, tout comme les références fournies. De soi-disant représentants de «gouvernements» étrangers ont en effet demandé à des entrepreneurs canadiens de leur donner des numéros de comptes bancaires dans le but d'y faire virer des fonds. Ils n'en ont évidemment rien fait, et ils ont plutôt effectué des retraits.

Des étrangers peuvent aborder les gens d'affaires lors de foires commerciales internationales sous prétexte d'acheter leur technologie. Ils cherchent souvent, en réalité, à obtenir des renseignements détaillés sur l'organisation de l'entreprise, sa technologie ou ses programmes de recherche et de développement. Ne perdez pas de vue les

informations et la technologie que vous emportez à une foire. Mettez-les en sécurité quand vous répondez à d'autres demandes de renseignements. Prenez note de toute demande suspecte ou inhabituelle. Ces détails peuvent se révéler précieux lorsque vous mettrez d'autres hommes ou femmes d'affaires en garde contre certains dangers potentiels.

Les hôtels

Une fois à l'étranger, il faut tenir pour acquis que ni les chambres d'hôtel, ni les salles de conférence, ni les bureaux des entreprises ne sont sûrs et qu'il ne faut pas y discuter de sujets confidentiels. Les mesures de sécurité y sont inadéquates. N'y laissez donc pas vos documents ou votre ordinateur portatif sans surveillance. Les téléphones peuvent avoir été mis sur écoute et les pièces peuvent être surveillées. Quelqu'un peut en outre y entrer subrepticement et la fouiller. Ne jetez ni bouts de papier ni bribes d'informations dans les corbeilles. Quelqu'un pourrait les prendre et obtenir ainsi des renseignements sur le déroulement de négociations commerciales d'affaires ou des contacts d'affaires. Enfin, les coffres-forts des hôtels ne sont pas nécessairement à l'abri des services de renseignements étrangers.

Les communications

De nombreux pays disposent de puissants moyens d'interception électroniques grâce auxquels ils peuvent intercepter les communications internationales transmises par satellites. Deux employés l'un en poste au siège social de l'entreprise et l'autre à l'étranger, peuvent néanmoins, au besoin, parler affaires ou s'envoyer des messages par télécopieur en toute sécurité en utilisant un nombre limité de mots et de codes prédéterminés. Les systèmes de chiffrage des communications téléphoniques et par télécopieur accroissent évidemment la sécurité des transmissions, mais ils n'offrent néanmoins pas de protection absolue contre les services secrets étrangers.

Les ordinateurs

Les ordinateurs et les communications électroniques font aujourd'hui partie intégrante de la panoplie indispensable aux gens d'affaires et aux fonctionnaires. Ils permettent de mémoriser, de transmettre, de récupérer et d'analyser d'énormes quantités d'informations et de données techniques. L'Internet et le *World Wide Net* jouent un rôle de plus en plus important en donnant accès à l'autoroute de l'information. Ces réseaux deviennent dès lors eux aussi des cibles vulnérables. Il est possible d'avoir accès à distance, n'importe où dans le monde, par l'intermédiaire des lignes de communication internationales, aux informations emmagasinées dans un ordinateur. Les signaux émis peuvent en effet être interceptés et décodés. Les pirates informatiques peuvent pénétrer dans les bases de données publiques comme privées. La technologie moderne permet même de récupérer des renseignements qui ont été effacés de la mémoire d'un ordinateur.

Conclusion

La vigueur économique d'un pays est en partie fonction de la santé de ses entreprises et de leur capacité à s'imposer sur le marché mondial. Il est tout aussi essentiel pour un pays de renforcer et de protéger sa force économique que de se défendre. Voilà pourquoi certains d'entre eux et leurs entreprises d'État estiment plus commodes de demander à leurs services de renseignements de faire de l'espionnage économique contre des entreprises et des personnes bien précises.

Il est vrai que dans la plupart des cas, les transactions des Canadiens à l'étranger se déroulent sans incident. Il n'en demeure pas moins important de reconnaître que la tentation de fausser les règles du jeu augmente à mesure que les enjeux économiques montent. Le présent document veut mettre les gens d'affaires canadiens en garde contre cette possibilité et leur donner les moyens d'y faire face.

avril 1998

N'hésitez pas à nous faire part de vos commentaires sur ce bulletin. Veuillez les adresser au coordonnateur national des questions de sécurité économique et de l'information, C.P. 9732, Succursale postale «T», Ottawa, K1G 4G4, téléphone (613) 231-0100, télécopieur (613) 842-1390. Si vous souhaitez discuter d'une question particulière, veuillez communiquer avec le coordon-nateur des questions de sécurité économique et de l'information de l'un des bureaux régionaux suivants du SCRS :

Terre-Neuve ..... (709) 772-5449

Nouvelle-Écosse ..... (902) 420-5900

Nouveau-Brunswick ..... (506) 452-3786

Québec
- Montréal ..... (514) 393-5600
- Québec ..... (418) 529-8926

Ontario
- Ottawa ..... (613) 998-1679
- Toronto ..... (416) 865-1480

Manitoba ..... (204) 983-5405

Saskatchewan ..... (306) 780-5512

Alberta
- Edmonton ..... (403) 421-5800
- Calgary ..... (403) 292-5255

Colombie-Britannique ..... (604) 528-7400